UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Xcedex, Inc., and Bababa Software, Inc.,

Plaintiffs,

v.

VMware, Inc.,

Defendant.

Civ. No. 10-3589 (PJS/JJK)

REPORT AND RECOMMENDATION

Andrea C. Wiltrout, Esq., and Tiffany A. Blofield, Esq., Winthrop & Weinstine, P.A. for Plaintiffs Xcedex, Inc., and Bababa Software, Inc.

Timothy J. Cruz, Esq., Faegre & Benson LLP, counsel for Defendant VMware, Inc.

This matter is before the Court on the motion of Defendant VMware, Inc., to dismiss Count III of Plaintiffs' Amended Complaint pursuant to Fed. R. Civ. P. 12(b)(6). (Doc. No. 27.) The case has been referred to this Court for a Report and Recommendation pursuant to 28 U.S.C. § 636 and D. Minn. Loc. R. 72.1 and 72.2. For the reasons set forth below, this Court recommends that the motion be granted.

BACKGROUND[1]

Plaintiff Xcedex, Inc. ("Xcedex") is a "virtualization planning and deployment software firm" that is "the leading provider of software products and services which help organizations with virtualization planning, energy savings, and device infrastructure analysis, including device inventory, applications, configuration and utilization for delivering action-oriented plans that enable the rapid identification and implementation of efficiency and cost saving measures." (Doc. No. 25, Am. Compl. ¶¶ 7, 12.) Defendant VMware, Inc. ("VMware") is "a public company which is the global leader in cloud infrastructure (i.e., internet-based computing whereby shared resources, software, and information are provided to computers and other devices on demand, like the electricity grid) and delivers customer-proven virtualization solutions to significantly reduce IT complexity." (*Id.* ¶ 9.)

One of Xcedex's assets is the X_Factor device intelligence software product, which features an "agent-less architecture." (*Id.* ¶ 13.) The X_Factor product "allows an organization's entire device infrastructure, including any

[1] This description of the case is taken from the Plaintiffs' Amended Complaint and memoranda. As can be quickly observed, Plaintiffs' description of the case is riddled with technical jargon and language that would perhaps be understood by an IT department but presents a special challenge to one not immersed in the world of computers. It is unclear whether this difficulty arises from the fact that the lawyers who drafted the pleadings did not themselves understand the case and thus did not take the time and effort to try to make it intelligible to the average reader, or whether it is a clever way to obscure the failings of the case. Either way, the Amended Complaint is not a "short and plain statement" for relief.

device with an IP address, to be either easily scanned or ported (manually migrated), [allowing for the] gathering [of] critical information to be used for analysis." (*Id.* ¶ 14.) In other words, X_Factor "is the software used in connection with P2V [Physical to Virtual] migration to validate data and determine which of the devices are viable and suitable candidates for virtualization." (*Id.* ¶ 29.) The analysis provided through the use of this software is purportedly critical to determining whether a device infrastructure can migrate to the cloud.

X_Factor's data-collector component is called Collector_X. (*Id.* ¶ 32.) According to the Amended Complaint, Collector_X "is the most essential and pertinent portion of the valuation process that drives the success of a virtualization interface." (*Id.* ¶ 34.) Collector_X apparently interprets something called "Snapshot."[2] (*Id.* ¶ 33.) The X_Factor analysis, however, can be used with or without Collector_X. (*Id.* ¶ 34.)

On April 1, 2006, Xcedex and VMware entered into a Professional Services Subcontractor Agreement (the "Agreement"). (*Id.* ¶ 17.) This Agreement provided terms regarding many types of future work orders, including

[2] The Amended Complaint explains that Infrastructure Solutions, Inc. ("ISI") was the original equipment manufacturer of Snapshot, and Xcedex has a license agreement with ISI for the use of Snapshot. (*Id.* ¶ 33.) Plaintiff Bababa Software, Inc. ("Bababa") is a corporation that has purchased certain assets from ISI, including all of the intellectual property rights held by ISI in certain "Snapshot" software. (*Id.* ¶ 8.)

a work order "authorizing VMware to access and use Xcedex's independently developed software platform (*i.e.*, the X-Factor Suite)[.]" (*Id.* ¶ 19.)

Sometime thereafter, NetApp, Inc. retained VMware to provide Thomson Reuters Applications Inc. ("Thomson") with Physical to Virtual ("P2V") migration services for 4,000 devices. (*Id.* ¶ 21.) In early 2009, VMware and Xcedex entered into a contract/work order ("the 2009 Work Order") in connection with this project concerning Thomson. (*Id.* ¶¶ 22, 23.) According to the Amended Complaint, the 2009 Work Order "provided that Xcedex would provide consulting services to assist VMware with the setup of the P2V migration factory[,]" and "confirmed that Xcedex would deliver authorization to access and use its X_Factor software as a service" but limited such access and use to "4,000 devices and licenses." (*Id.* ¶¶ 26, 27.) Thompson instructed Xcedex to not use Collector_X to scan devices from its Linux systems, but instead, Thomson used a tool that it had called Performance Statistics to gather the data for Linux-based systems. (*Id.* ¶ 37.) The data collected using Performance Statistics was then imported into X-Factor for analysis. (*Id.* ¶ 38.)

According to the Amended Complaint, VMware also asked that Thomson's data be manually migrated rather than scanned per the work order. (*Id.* ¶ 44.) Xcedex alleges that the reason why VMware wanted the data manually migrated was "so that it could subvert the Contract by requesting data directly from Xcedex's supplier." (*Id.* ¶ 45.) The Amended Complaint is silent about what type of "data" VMware requested from Xcedex's supplier. Apparently the requested data had something to do with additional analysis of the Thompson servers because Xcedex alleges in the next paragraph that VMware "instructed its employees—who were former Xcedex employees and/or independent contractors—to contact Xcedex's supplier, ISI, directly" so that it could "obtain additional licenses and devices in excess of the 4,000 it had contracted for with Xcedex[.]" (*Id.* ¶ 46.) These former Xcedex employees and/or independent contractors allegedly had confidentiality and nondisclosure agreements with Xcedex that covered "the information used by them to unlawfully obtain X_Factor licenses[.]" (*Id.* ¶ 47; *see also* ¶ 48 (referencing one such agreement signed by one Dustin Haugen in 2004).) Xcedex asserts that "[b]y going around Xcedex, and in contravention of the Subcontractor Agreement and the Work Orders, VMware was able to obtain in excess of 16,700 additional licenses for devices." (*Id.* ¶ 50.) Because VMware allegedly then had accessed over 4,000 licenses for Snapshot, ISI contacted Xcedex to obtain "a true up," which then allegedly forced Xcedex to enter into a new agreement with ISI in April 2010 with less favorable terms. (*Id.* ¶¶ 51, 52.) Xcedex also alleges that –

> VMware's actions have impaired the integrity of Xcedex's computer systems, causing Xcedex to suffer damages and losses in connection with investigation as well as implementation of corrective measures to prevent further damage, as well as loss of revenue and other losses and damages in an amount to be proved at trial, but in any event, an amount well over $5,000 aggregated over a one-year period.

(*Id.* ¶ 79.)

DISCUSSION

I. Standard of Review

Federal Rule of Civil Procedure 8 requires that a complaint present "a short and plain statement of the claim showing that the pleader is entitled to relief." A civil complaint will be dismissed for "failure to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). To state a cause of action that will survive a Rule 12(b)(6) motion, a complaint must allege a set of historical facts, which, if proven true, would entitle the plaintiff to some legal redress against the named defendant(s) under some established legal theory. *Martin v. Aubuchon*, 623 F.2d 1282, 1286 (8th Cir. 1980) (noting that "the complaint must allege facts, which if true, state a claim as a matter of law").

In deciding a motion to dismiss, a court assumes all facts in the complaint to be true and construes all reasonable inferences from those facts in the light most favorable to the complainant. *Morton v. Becker*, 793 F.2d 185, 187 (8th Cir. 1986). But in so doing, a court need not accept as true wholly conclusory allegations, *Hanten v. Sch. Dist. of Riverview Gardens*, 183 F.3d 799, 805 (8th Cir. 1999), or legal conclusions drawn by the pleader from the facts alleged. *Westcott v. City of Omaha*, 901 F.2d 1486, 1488 (8th Cir. 1990).

To survive a motion to dismiss, a complaint must contain "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A complaint states a plausible claim for relief if its "factual content . . . allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1949 (2009). Although a complaint need not contain "detailed factual allegations," it must contain facts with enough specificity "to raise a right to relief above the speculative level." *Twombly*, 550 U.S. at 555.

II. Motion to Dismiss Count III

Count III of the Amended Complaint alleges that VMware's actions, as described above, constitute violations of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a).[3] Specifically, Plaintiffs claim that VMware violated subsections (a)(4), (a)(5)(B), and (a)(5)(C). (Am. Compl. ¶¶ 74–76.) VMware argues that Plaintiffs' claims under the CFAA must be dismissed for failure to state claims on which relief can be granted.

The CFAA, which is primarily a criminal statute involving computer-hacking-related activities, extends a private cause of action under § 1030(g), which states in relevant part:

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i).[4]

[3] All references to the CFAA are to the 2008 version.

[4] Prior to the 2008 amendments, these factors were set forth in subsection (a)(5)(B).

18 U.S.C. § 1030(g).[5] Plaintiffs have brought their claims under § 1030(a)(4), (a)(5)(B), and (a)(5)(C). Those subsections state the following:

> (a) Whoever - -
>
> . . . .
>
> (4) knowingly and with intent to defraud, accesses a protected computer[6] without authorization, or exceeds authorized

[5] VMware argues that § 1030(g) limits civil actions under the CFAA to violations of subsection (a)(5) and therefore Plaintiff's claim under subsection (a)(4) should be dismissed. VMware cites *Cenveo Corp. v. CelumSolutions Software GMBH & Co. KG*, 504 F. Supp. 2d 574, 580 (D. Minn. 2007), and *McLean v. Mortgage One & Fin. Corp.*, No. Civ. 04-1158, 2004 WL 898440, at *2 (D. Minn. 2004), in support. Other courts, however, have found that the CFAA authorizes a civil cause of action for violations of any of the subsections of § 1030(a). *See Fiber Sys. Int'l, Inc. v. Roehrs*, 470 F.3d 1150, 1156–57 (5th Cir. 2006) (rejecting the argument that § 1030(g) authorizes civil actions only for violations of subsection (a)(5) and holding that the CFAA authorizes a civil action for violations of the other subsections of § 1030(a), so long as one of the five factors referenced in § 1030(g) is "involved"); *P.C. Yonkers, Inc. v. Celebrations! The Party & Seasonal Superstore, LLC*, 428 F.3d 504, 511 (3d Cir. 2005) ("We do not read [§ 1030(g)] . . . as limiting relief to claims that are entirely based only on subsection (a)(5), but, rather, as requiring that claims brought under other [sub]sections must meet, in addition, one of the five number (a)(5)(B) 'tests.'"); *Theofel v. Farey-Jones*, 359 F.3d 1066, 1078 (9th Cir. 2003) (holding that § 1030(g) "applies to any violation of 'this section' and, while the offense must involve one of the five factors in (a)(5)(B), it need not be one of the three offenses in (a)(5)(A)"). And the CFAA was amended in 2008, listing the factors that were previously set forth in subsection (a)(5)(B), now in subsection (c)(4)(A)(i). The Eighth Circuit has yet to address the issue whether a civil action can be brought under subsection (a)(4). This Court need not address the issue here, however, because even assuming a civil action can be brought under subsection (a)(4), this Court concludes, as explained below, that Plaintiffs have failed to allege sufficient facts to support any of their claims asserted in Count III of the Amended Complaint.

[6] The term "protected computer" is defined by the CFAA, in relevant part, as a computer "which is used in or affecting interstate or foreign commerce or

(Footnote Continued on Next Page)

> access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;
>
> (5) . . .
>
> (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
>
> (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

18 U.S.C. § 1030(a)(4), (a)(5)(B), and (a)(5)(C). Violations of those subsections therefore require allegations that VMware accessed Xcedex's computer's without authorization (or in excess of authorized access with respect to subsection (a)(4)).

Plaintiffs concede in the Amended Complaint that Xcedex authorized VMware to use X_Factor software to assist in the analysis of 4,000 Thompson servers. Specifically, when Xcedex and VMware entered into their Agreement, they provided terms for a future work order "authorizing VMware to access and use Xcedex's independently developed software platform (*i.e.*, the X-Factor Suite)[.]" (Am. Compl. ¶ 19.) Then later, a 2009 Work Order specifically stated that –

(Footnote Continued from Previous Page)
communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States[.]" 18 U.S.C. § 1030(e)(2).

> Subcontractor [Xcedex] will deploy and implement on or before the start of the project, X-Factor software for 4000 devices to be utilized for design validation, analysis, capacity planning and P2V work flow automation.

(Am. Compl. ¶ 28 (emphasis removed).) According to the Amended Complaint, the 2009 Work Order "confirmed that Xcedex would deliver authorization to access and use its X_Factor software as a service" but limited such access and use to "4,000 devices and licenses." (*Id.* ¶¶ 26, 27.) Plaintiffs do not directly address whether VMware was without authorization or exceeded its authorized access, but in their argument regarding whether damages were properly plead, Plaintiffs assert the theory that Xcedex controlled the number of available device licenses for the X-Factor through a component supplied by a company named ISI, and that these controls could be overrun through the use of a password given only to certain Xcedex employees. Plaintiffs assert that VMware, through the use of a password, subverted the controls that X_Factor had in place, and therefore VMware was able to download thousands of additional licenses. (Doc. No. 34, Pl.'s Mem. in Opp'n to Mot. to Dismiss Count III of the Am. Compl. 24.)[7]

There is a split among courts on the question of whether a party who has accessed computer information that it was otherwise permitted to access, and has done so with an improper purpose, has accessed a computer "without

[7] Notably, no reference to this "password" theory is mentioned in the facts alleged to support Plaintiff's FCAA claim. The allegations regarding the use of a password appear at paragraphs 90–95, in support of Plaintiff's misappropriation-of-trade-secrets claim.

authorization" or "exceed[ed] authorized access" and therefore may be held civilly liable under the CFAA. *Compare, e.g.*, *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420–21 (7th Cir. 2006) (concluding that an employee may act "without authorization" or "in excess of authorized access" when he accesses confidential or proprietary business information from his employer's computers that he has permission to access but then uses that information in a manner that is inconsistent with the employer's interests or in violation of contractual obligations or fiduciary duties), *with e.g.*, *Lockheed Martin Corp. v. Speed*, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *5 (M.D. Fla. Aug. 1, 2006) (concluding that the CFAA is implicated only by the unauthorized access, obtainment, or alteration of information, not the misuse or misappropriation of information obtained with permission); *see also Condux Int'l v. Haugum*, Civil No. 08-4824 (ADM/JSM), 2008 WL 5244818 (D. Minn. Dec. 15, 2008) (citing cases). This Court agrees with the court in *Condux Int'l v. Haugum*, that the *Lockheed* line of cases, which provide a narrower interpretation, reflects a more accurate interpretation of the meaning of the terms "without authorization" and "exceeds authorized access." *See Condux*, 2008 WL 5244818, at *4. Further, the CFAA itself defines "exceeds authorized access" as "access[ing] a computer with authorization and [using] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). Therefore, "without authorization" and "exceed[ing] authorized access" depend on the "unauthorized use of *access*," not on the "unauthorized use of *information*." *Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007) (emphasis added); *see also Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008) ("[T]he plain language of [subsections (a)(2), (a)(4), and (a)(5)(A)(ii) and (iii)] target unauthorized procurement or alteration of information, not its misuse or misappropriation.") (quotations omitted); *Condux*, 2008 WL 5244818, at *5 (citing legislative history).[8]

The Amended Complaint does not explain whether VMware ever accessed Xcedex's computer at all, much less whether there was any improper accessing or hacking into Xcedex's computer by VMware.[9] The conduct prohibited by the CFAA is "analogous to that of 'breaking and entering' rather than using a computer . . . in committing the offense." *Condux*, 2008 WL 5244818, at *5 (quoting H.R. Rep. No. 98-894, at 20 (1984). At one point, the Amended

[8] Several courts have noted that this interpretation of the statute is supported by the rule of lenity. *See, e.g.*, *US Bioservices Corp. v. Lugo*, 595 F. Supp. 2d 1189, 1194 n.5 (D. Kan. 2009) (citing cases). When a court is confronted with two rational readings of a criminal statute, it is required to construe the statute in favor of the defendant. *See United States v. Santos*, 553 U.S. 507, 514 (2008). This rule of lenity applies to civil statutes that have criminal applications because courts are required to interpret such statutes consistently, regardless of whether the court encounters the statute in a criminal or noncriminal context. *Clark v. Martinez*, 543 U.S. 371, 380 (2005).

[9] The term "computer" is defined in the CFAA as meaning "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device[.]" 18 U.S.C. § 1030(e)(1).

Complaint states that VMware wanted Thomson's data to be manually migrated rather than scanned per the work order. (*Id.* ¶ 44.) The Amended Complaint does not say whether this "data" was collected from Xcedex's or Thompson's computers. But even if the data were collected from Xcedex's computers, this hardly seems to involve unauthorized hacking into Xcedex's computers. As best this Court can determine from the Amended Complaint, that data was collected pursuant to an authorization called a "Work Order Project Change Request," whereby "VMware asked for 'Thomson Reuters legacy migration and data collection data ported over to Nomad Tool.'" (*Id.* ¶ 44.)

The Amended Complaint also states that VMware obtained "in excess of 16,700 additional licenses for devices" from or through a company named ISI, which is described as Xcedex's "supplier," presumably of software. (*Id.* ¶ 50.) The Amended Complaint, however, provides no information about any relationship between the act of obtaining these additional licenses directly from ISI and accessing Xcedex's computers. All that the Amended Complaint alleges is that "ISI contacted Xcedex to obtain a true up as VMware had accessed over 4,000 licenses for Snapshot." (*Id.* ¶ 51.) Whatever this means, it does not provide a sufficient basis to conclude that Xcedex has a plausible claim that the locus of VMware's alleged misconduct was Xcedex's computer. As explained by the court in *Brett Senior & Associates, P.C. v. Fitzgerald*:

> [T]he point of the access requirement, as explained by the Senate Committee, is to ensure that the use of the computer is integral to the perpetration of a fraud, in contrast to the more expansive

> definitions of mail and wire fraud . . . . In the plaintiff's reading, however, the computer is not the locus of the wrongful conduct, but merely the fortuitous place where the information was obtained.

No. 06-1412, 2007 WL 2043377, at *4 (E.D. Pa. July 13, 2007). The court continues:

> Under the plaintiff's view, turning over information to a competitor would be a violation of the CFAA if obtained from a computer but not, for example, from a wastebasket, even though the defendant was permitted to access the information in the computer.

Id. at n. 7. Because nothing in the Amended Complaint shows that Xcedex has a plausible claim that VMware engaged in computer hacking in violation of the CFAA, Xcedex's claims under the CFAA should be dismissed.[10]

In conclusion, the facts alleged in the Amended Complaint appear to more properly support claims for breach of contract, misappropriation of trade secrets, tortious interference with a contract, or tortious interference with contractual and business relationships, which are all causes of action pleaded in the Amended

[10] Because this Court concludes that Plaintiffs Amended Complaint should be dismissed on the above grounds, this Court does not address whether Plaintiffs have properly pleaded damages and/or losses under the CFAA. This Court notes, however, that Plaintiffs have only parroted the definition of "damage" and "loss" set forth in the CFAA, with conclusory allegations, including that Xcedex was forced to enter into a new agreement with ISI in April 2010 with less favorable terms. No facts are pled that explain what the less favorable terms were, nor are any facts pleaded explaining how the integrity of Xcedex's computer systems were impaired, or what was expended in connection with the investigation or corrective measures. *See Iqbal*, 129 S. Ct. at 1949 (stating that "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements," will not pass muster under *Twombly*).

Complaint, are not subject to Defendant's motion to dismiss, and thus survive at this stage in the case.

RECOMMENDATION

Based on the foregoing and all of the files, records, and proceedings herein, **IT IS HEREBY RECOMMENDED** that:

1. Defendants' Motions to Dismiss (Doc. No. 27), be **GRANTED**.

Date: June 8, 2011

s/ Jeffrey J. Keyes
JEFFREY J. KEYES
United States Magistrate Judge

Under Local Rule 72.2(b) any party may object to this Report and Recommendation by filing with the Clerk of Court, and serving all parties by **June 22, 2011,** a writing which specifically identifies those portions of this Report to which objections are made and the basis of those objections. Failure to comply with this procedure may operate as a forfeiture of the objecting party's right to seek review in the Court of Appeals. A party may respond to the objecting party's brief within **fourteen days** after service thereof. All briefs filed under this rule shall be limited to 3500 words. A judge shall make a de novo determination of those portions of the Report to which objection is made. This Report and Recommendation does not constitute an order or judgment of the District Court, and it is therefore not appealable directly to the Circuit Court of Appeals.

Unless the parties stipulate that the District Court is not required by 28 U.S.C. § 636 to review a transcript of the hearing in order to resolve all objections made to this Report and Recommendation, the party making the objections shall timely order and file a complete transcript of the hearing within **ten days** of receipt of the Report.